

## **AMENDMENTS TO THE CLAIMS**

The listing of claims replaces all prior versions, and listings, of claims in the application:

### **Listing of Claims:**

1. (Original) A method comprising:  
receiving an audiovisual master file from a movie recording studio or other organization containing an audiovisual presentation such as a to-be-released or recently released movie, the audiovisual master file being in a first encoded and compressed format;  
adding watermark characters to the encoded audiovisual master file;  
adding camera artifacts to the encoded audiovisual master file;  
encrypting the encoded audiovisual master file to create an encrypted encoded audiovisual master file;  
generating keys associated with the encrypted encoded audiovisual master file for using in decoding the encrypted encoded audiovisual master file;  
transmitting the encrypted encoded audiovisual master file and the associated keys to a distribution point host computer;  
loading the transmitted encrypted encoded audiovisual master file on the distribution point host computer;  
linking the distribution point host computer with a self-contained entertainment device and establishing bidirectional authentication between the distribution point host computer and the self-contained entertainment device through use, in part, of an input-output of the self-contained entertainment device;  
after bi-directional authentication occurs, using the distribution point host computer to delete at least some of the previously loaded encrypted encoded audiovisual master files from the self-contained entertainment device;  
using the distribution point host computer to transfer the newly loaded encrypted encoded audiovisual master file and keys associated with the newly loaded encrypted encoded audiovisual master file to the self-contained entertainment device to which the distribution point host computer is linked without decryption of the

newly loaded encrypted encoded audiovisual master file being transferred to the self-contained entertainment device; and  
storing the newly loaded encrypted encoded audiovisual master file and the keys associated with the newly loaded encrypted encoded audiovisual master file on an encrypted hard drive of the self-contained entertainment device to which the distribution point host computer is linked.

2. (Original) The method of claim 1 further including using the self-contained entertainment device to subsequently decrypt the newly loaded encrypted encoded audiovisual master file stored on an encrypted hard drive of the self-contained entertainment device using the keys associated with the newly loaded encrypted encoded audiovisual master file stored on an encrypted hard drive of the self-contained entertainment device to display audiovisual presentation of the newly loaded encrypted encoded audiovisual master file stored on an encrypted hard drive of the self-contained entertainment device to a person who rented the self-contained entertainment device.

3. (Currently Amended) A system comprising:  
a sound output;  
a visual display;  
a processor;  
encrypted audiovisual files;  
an encrypted hard drive containing the encrypted audiovisual files;  
a hard drive decryptor configured for decrypting the encrypted hard drive;  
a file decryptor for decrypting the encrypted files;  
an input-output with a unique physical configuration;  
an input-output authenticator configured to authenticate a device attempting to communicatively link to the input-output;  
a case being secured with anti-tamper fasteners; and  
an evidentiary seal positioned to rupture when a portion of the case is disassembled.

4. (Original) A method comprising:
  - receiving an audiovisual master file from a movie recording studio or other organization containing an audiovisual presentation such as a to-be-released or recently released movie, the audiovisual master file being in a first encoded and compressed format;
  - encrypting the encoded audiovisual master file to create an encrypted encoded audiovisual master file;
  - generating keys associated with the encrypted encoded audiovisual master file for using in decoding the encrypted encoded audiovisual master file;
  - transmitting the encrypted encoded audiovisual master file and the associated keys to a distribution point host computer;
  - loading the transmitted encrypted encoded audiovisual master file on the distribution point host computer;
  - linking the distribution point host computer with a self-contained entertainment device and establishing bi-directional authentication between the distribution point host computer and the self-contained entertainment device through use, in part, of an input-output of the self-contained entertainment device;
  - after bi-directional authentication occurs, using the distribution point host computer to delete at least some of the previously loaded encrypted encoded audiovisual master files from the self-contained entertainment device;
  - using the distribution point host computer to transfer the newly loaded encrypted encoded audiovisual master file and keys associated with the newly loaded encrypted encoded audiovisual master file to the self-contained entertainment device to which the distribution point host computer is linked without decryption of the newly loaded encrypted encoded audiovisual master file being transferred to the self-contained entertainment device; and
  - storing the newly loaded encrypted encoded audiovisual master file and the keys associated with the newly loaded encrypted encoded audiovisual master file on an encrypted hard drive of the self-contained entertainment device to which the distribution point host computer is linked.

5. (Original) A system comprising:  
a sound output;  
a visual display;  
a processor;  
encrypted audiovisual files;  
an encrypted hard drive containing the encrypted audiovisual files;  
a hard drive decryptor configured for decrypting the encrypted hard drive;  
a file decryptor for decrypting the encrypted files; and  
an input-output authenticator configured to authenticate a device attempting to  
communicatively link to the input-output.
6. (New) The method of claim 1, wherein adding watermark characters to the  
encoded audio visual master file includes adding characters identifying time and place of  
encoding.
7. (New) The method of claim 1, wherein adding camera artifacts to the encoded  
audiovisual master file includes adding elements invisible to the naked eye upon display of the  
audiovisual master file, but visible to the naked eye upon display of a video recording of the  
audiovisual master file.
8. (New) The system of claim 1, wherein the system is an in-flight entertainment  
device for use during a commercial airline flight.
9. (New) The system of claim 3, wherein the display, processor and encrypted hard  
drive are integral in a single portable device.
10. (New) The system of claim 3, wherein the hard drive decryptor and file decryptor  
are on a same physical device.

11. (New) The system of claim 10, wherein the hard drive decryptor is configured to use decryption methods separate from those used by the file decryptor to decrypt individual encrypted files.

12. (New) The system of claim 3, wherein the input-output is on an in-flight entertainment device and the unique physical configuration includes a shape complementary to a shape of a uniquely formed connector configured to physically couple the in-flight entertainment device to a distribution point host computer.

13. (New) The system of claim 12, wherein the unique physical coordination is configured to communicate through a standard communication protocol.

14. (New) The system of claim 13, wherein the standard communication protocol includes at least one of USB 2.0 or IEEE 1394.

15. The system of claim 3, wherein the input-output is configured to provide a sole and exclusive source for external access to the encrypted hard drive.

16. (New) The system of claim 3, wherein the input-output authenticator is configured to authenticate the device attempting to communicatively link to the input-output only during a limited time window.

17. (New) The system of claim 16, wherein the input-output authenticator is configured to require a physical reconnection between the device and the input-output when authentication is attempted outside of the limited time window.

18. (New) The system of claim 5, wherein the system includes an in-flight entertainment device and the device attempting to communicatively link to the input-output is a distribution point computer, and wherein the in-flight entertainment device is configured to display the decrypted audiovisual files on the visual display after disconnection from the distribution point host computer.

19. (New) The system of claim 18, wherein the in-flight entertainment device is configured for use during a commercial airline flight, separate from the distribution point host computer.